

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **FOR THE WESTERN DISTRICT OF WASHINGTON**
10 **AT SEATTLE**

11 LYNNE BURKHARDT, individually, and on
12 behalf of all others similarly situated,

13 Plaintiff,

14 vs.

15 PREMERA BLUE CROSS, a Washington
16 nonprofit corporation; and DOES 1-50,

17 Defendants.

Case No.: _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

18 Plaintiff LYNNE BURKHARDT ("Plaintiff"), by and through her counsel, brings this
19 Class Action Complaint against Defendant Premera Blue Cross on behalf of herself and all
20 others similarly situated, and alleges, upon personal knowledge as to her own actions and her
21 counsel's investigations, and upon information and belief as to all other matters, as follows:

22 **PARTIES**

23 1. Defendant Premera Blue Cross ("Defendant") is a Washington nonprofit
24 corporation with headquarters located at 7001 220th Street SW, Mountlake Terrace,
25 Washington, 98043. conducts business throughout this District and the United States.

26 2. Plaintiff LYNNE BURKHARDT ("Plaintiff") is an individual and currently a
resident of Gig Harbor, Washington, who is insured through Defendant.

CLASS ACTION COMPLAINT - 1

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

3. Plaintiff is unaware of the true names and capacities of the defendants sued as DOES 1-50, and therefore sues these defendants by fictitious names. Plaintiff will seek leave to amend this Complaint when and if the true identities of these DOE defendants are discovered. Plaintiff is informed and believes and thereon alleges that each of the Defendants designated as a DOE is responsible in some manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby proximately caused injuries and damages to Plaintiff as herein alleged, and is thus liable for the damages suffered by Plaintiff.

JURISDICTION AND VENUE

4. This Court has original jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action in which (i) the proposed class consists of more than 100 members; (ii) at least some members of the proposed class are citizens of a state different from any defendant; and (iii) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendant because Defendant is authorized to, and does, business in the State of Washington, providing health insurance to citizens of this State such as Plaintiff.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because Defendant resides in this District and a substantial part of the events that give rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

7. In what appears to be the largest data breach reported to date involving patient medical information, health insurer Premera Blue Cross (“Defendant”), through its deficient cyber security, exposed medical data and financial information of 11 million of its insureds and customers.

8. As a result of Defendant’s deficient security, hackers appear to have gained access to claims data, including clinical information, along with banking account numbers,

1 Social Security numbers, birth dates, a variety of personally identifiable information (“PII”), and
 2 other data in an attack that began at least as early as May 2014 (the “Data Breach”).

3 9. By May 5, 2014, hackers infiltrated Defendant’s Information Technology (“IT”) system and, for months thereafter, had access to as many as 11 million records of current and
 4 former insureds and employees, as well as Blue Cross Blue Shield customers who received
 5 medical treatment in Washington or Alaska. The hackers were able to access these individuals’
 6 names, dates of birth, email addresses, addresses, telephone numbers, Social Security numbers,
 7 member identification numbers, bank account information, claims information including clinical
 8 data, and other information.

9 10. Defendant has stated that the Data Breach affected current and former customers
 10 of Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliates, including
 11 Vivacity and Connexion Insurance Solutions, Inc. Several days after the breach, LifeWise
 12 Health Plan of Oregon announced that 60,000 of its members were compromised by the Data
 13 Breach.

14 11. Defendant further acknowledged that the breach affected members of any Blue
 15 Cross Blue Shield plan who had received medical treatment in Washington or Alaska, and that
 16 “[i]ndividuals who do business with us and provided us with their email address, personal bank
 17 account number or social security number are also affected.”

18 <<http://www.premeraupdate.com/>> (statement of Jeffrey Roe) (last visited Mar. 30, 2015).

19 12. On information and belief, Defendant failed to properly segregate medical
 20 information from other PII and financial information.

21 13. The federal government explicitly warned Defendant that its cyber security
 22 systems were vulnerable before the Data Breach occurred. On April 18, 2014, the Office of
 23 Personnel Management delivered the results of an audit it performed on Premera’s IT systems.
 24 The audit identified ten areas in which Defendant’s systems were inadequate and vulnerable to
 25 attack. See Mike Baker, *Feds Warned Premera About Security Flaws Before Breach*, SEATTLE
 26

1 TIMES, Mar. 18, 2015, *available at* <[http://www.seattletimes.com/business/local-business/feds-](http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/)
2 [warned-premera-about-security-flaws-before-breach/](http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/)> (last visited Mar. 30, 2015).

3 14. The audit found that Premera was not implementing critical security patches and
4 other software updates and warned: “Failure to promptly install important updates increases the
5 risk that vulnerabilities will not be remediated and sensitive data could be breached.” U.S.
6 Office of Personnel Management, Office of the Inspector General, *Final Audit Report* at 7 (Nov.
7 8, 2014), *available at* <[https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/](https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf)
8 [opm-audit.pdf](https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf)> (last visited Mar. 30, 2015).

9 15. Instead of responding to the federal audit, implementing the Inspector General’s
10 recommendations, and immediately strengthening its IT security, Defendant allowed itself to
11 remain vulnerable and, predictably, allowed the Data Breach to occur months after the federal
12 audit was completed.

13 16. The hackers appear to have accessed the PII and medical information in
14 unencrypted form, or to have obtained a key allowing the information to be unencrypted. *See,*
15 *e.g.,* Joseph Goedert, *Premera Breach Highlights Need for Encryption*, HealthData
16 Management, Mar. 19, 2015, *available at* <[http://www.healthdatamanagement.com/news/](http://www.healthdatamanagement.com/news/Decision-to-Forgo-Encryption-Costing-Health-Organizations-Dearly-50014-1.html)
17 [Decision-to-Forgo-Encryption-Costing-Health-Organizations-Dearly-50014-1.html](http://www.healthdatamanagement.com/news/Decision-to-Forgo-Encryption-Costing-Health-Organizations-Dearly-50014-1.html)> (last visited
18 Mar. 30, 2015).

19 17. Medical records are highly valuable on underground criminal exchanges where
20 stolen data is sold because the information can be used to engage in insurance fraud, and
21 because the PII involved can be used to engage in a variety of other crimes, including financial
22 identity theft, for instance by using one’s social security number to open new accounts in a
23 victim’s name.

24 18. Defendant did not disclose the Data Breach until March 17, 2015, despite having
25 known about it since at least January 29, 2015, according to its own account of events.

26 19. Defendant has not yet fully and accurately informed its insureds regarding the
scope of the Data Breach or the risks of identity theft. It is not clear how many insureds

1 Defendant has notified to date, but Defendant itself estimates that it will not complete the
2 notification process until April 20, 2015 — approximately three months after the Data Breach.

3 20. It is critical that companies affected by data breaches provide timely, accurate,
4 and complete information to those whose information has been compromised so they can take
5 necessary precautions to protect themselves and their families from further harm. Accordingly,
6 the Health Insurance Portability and Accountability Act (“HIPAA”) requires that Defendant
7 provide notice without unreasonable delay and no later than 60 days after discovery of a breach.
8 *See* 45 C.F.R. § 164.404. Washington state law similarly requires Defendant to provide notice
9 in the most expedient time possible. *See* RCW § 19.255.010.

10 21. As a result of the Data Breach, Plaintiff and members of the Class will have to
11 take a variety of steps to monitor for and safeguard against identity theft and are at a much
12 greater risk of suffering such identity theft, which may well include fraudulent medical care in
13 the victims’ names, charges for such medical care, and/or adulteration of the victims’ true
14 medical records in possibly dangerous ways. In addition, these victims of the Data Breach are at
15 a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice
16 Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the
17 nation’s economy billions of dollars every year. *See* U.S. Dept. of Justice, Bureau of Justice
18 Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at*
19 <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Mar. 30, 2015).

20 22. Loss of social security numbers, such as those disclosed through the Data Breach
21 that Defendant failed to prevent, can be especially devastating, as thieves can use such
22 information, in combination with the other PII stolen, to open new accounts in victims’ names
23 without their knowledge, and even to obtain fraudulent encumbrances on such victims’ property.

24 23. Defendant breached its duty (a) to protect and safeguard its insureds’ PII and
25 medical information, and (b) to notify those affected in a timely and complete manner. Plaintiff
26 brings this action on behalf of herself and similarly situated insureds whose PII and medical
information was compromised in the Data Breach, for compensation for the injuries they have

suffered and for injunctive relief to ensure that Defendant takes proper security precautions in the future and gives prompt and full information to all affected people concerning their exposure in the Data Breach.

CLASS ACTION ALLEGATIONS

24. Plaintiff brings this action on behalf of a nationwide class preliminarily defined as:

All current or former insureds of Premiera Blue Cross residing in the United States whose personal and/or medical information was compromised in the data breach disclosed by Premiera Blue Cross on or about March 17, 2015.

(The “Nationwide Class.”) Excluded from the Nationwide Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

25. Plaintiff also brings this action on behalf of a Washington State Class, preliminarily defined as:

All current or former insureds of Premiera Blue Cross residing in the State of Washington whose personal and/or medical information was compromised in the data breach disclosed by Premiera Blue Cross on or about March 17, 2015.

(The “Washington Class.”) Excluded from the Washington Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

26. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party under Rule 23.

27. **Numerosity.** The proposed Nationwide Class consists of more than 11 million members—far too many to join in a single action, and although the Washington Class is smaller,

on information and belief the Washington Class consists of thousands of members, at a minimum, and also satisfies the numerosity requirement.

28. **Ascertainability.** Class members are readily identifiable from information in Defendant's possession, custody, or control.

29. **Typicality.** Plaintiff's claims are typical of class members' claims as each arises from the same Data Breach, the same alleged negligence of and/or statutory violations by Defendant, and the same unreasonable manner of notifying Defendant's insureds regarding the Data Breach.

30. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the all proposed classes. Her interests do not conflict with class members' interests and she has retained counsel experienced in complex class action litigation and medical data privacy to vigorously prosecute this action on behalf of both classes.

31. **Commonality.** Plaintiff's and class members' claims raise predominantly common factual and legal questions that can be answered for all class members through a single class-wide proceeding. For example, to resolve any class member's claims, it will be necessary to answer the following questions. The answer to each of these questions will necessarily be the same for each class member.

- a. Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal, financial, and/or other information;
- b. Whether Defendant unreasonably delayed in notifying affected individuals of the Data Breach and whether the belated notice was adequate;
- c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- d. Whether Defendant's conduct was negligent;

- e. Whether Defendant's conduct in connection with the Data Breach and notification thereof violated HIPAA;
- f. Whether Defendant's conduct in connection with the Data Breach and notification thereof violated Washington State law;
- g. Whether Defendant's conduct in connection with the Data Breach and notification thereof breached the terms of any implied and/or express contracts between it and Class members;
- h. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

32. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. The damages available to individual plaintiffs are insufficient to make litigation addressing Defendant's medical privacy practices economically feasible in the absence of the class action procedure.

33. In the alternative, class certification is appropriate because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the class as a whole.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and all Classes)

34. Plaintiff incorporates by reference all other paragraphs alleged herein.

35. Defendant required Plaintiff and class members to submit non-public PII and medical information in order to acquire coverage under a health insurance policy and/or receive medical treatment.

36. Defendant collected and stored this PII and medical information.

37. Defendant assumed a duty of care to use reasonable means to secure and

1 safeguard this PII and medical information, to prevent disclosure of the information, to guard the
2 information from theft, and to detect any attempted or actual breach of its IT systems.

3 38. Defendant breached its duty of care by failing to secure and safeguard the PII and
4 medical information of Plaintiff and other members of the classes. Defendant negligently
5 maintained systems that it knew were vulnerable to a security breach, despite being made aware
6 of these vulnerabilities any number of ways, including through the federal government's audit of
7 those very systems. Defendant negligently stored PII and medical information in an
8 unencrypted form on a single, highly vulnerable database.

9 39. Defendant continues to breach this duty of care by failing to share crucial,
10 complete information with Plaintiff and other members of the classes in a timely manner.

11 40. Plaintiff and the other members of the classes have suffered harm as a result of
12 Defendant's negligence. These victims' loss of control over the PII and medical information
13 exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft,
14 credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft.
15 Plaintiff and other members of the proposed classes suffered and continue to suffer further harm
16 by virtue of Defendant's failure to give timely and complete notice to them concerning the Data
17 Breach and the risks they face.

18 **SECOND CAUSE OF ACTION**

19 ***Negligence per se***

20 **(On Behalf of Plaintiff and all Classes)**

21 41. Plaintiff incorporates by reference all other paragraphs alleged herein.

22 42. Under HIPAA, Defendant had a duty to secure and safeguard the personal
23 information of its customers. Defendant acknowledged this duty to its customers in its Notice of
24 Privacy Practices, and warranted that it would comport with its duties under HIPAA.

25 43. Defendant violated HIPAA by failing to secure and safeguard the PII and medical
26 information belonging to Plaintiff and other members of the classes; by failing to implement
27 protections against "reasonably anticipated threats," 45 C.F.R. § 164.306; by failing to encrypt

1 the PII and medical information, 45 C.F.R. § 164.312; and by failing to notify Plaintiff and other
2 members of the classes in accordance with the requirements set forth at 45 C.F.R. § 164.404.

3 44. Defendant further violated notification requirements under state law, including
4 RCW § 19.255.010 and Or. Rev. Stat. § 646A.604, and state law that required Defendant to
5 properly safeguard Defendant's PII and medical information, including RCW § 19.255.020 and
6 Or. Rev. Stat. § 646A.622.

7 45. Plaintiff and the other members of the classes have suffered harm as a result of
8 Defendant's negligence *per se*. These victims' loss of control over the PII and medical
9 information exposed subjects each of them to a greatly enhanced risk of identity theft, medical
10 identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of
11 fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to
12 suffer further harm by virtue of Defendant's failure to give timely and complete notice to them
concerning the Data Breach and the risks they face.

13 **THIRD CAUSE OF ACTION**

14 **Bailment**

15 **(On Behalf of Plaintiff and all Classes)**

16 46. Plaintiff incorporates by reference all other paragraphs alleged herein.

17 47. Plaintiff and other members of the proposed classes delivered and entrusted their
18 PII and medical information to Defendant for the sole purpose of receiving health insurance
19 services and/or medical treatment from Defendant.

20 48. By delivering their PII and medical information to Defendant, Plaintiff and other
21 members of the proposed classes intended and understood that Defendant would safeguard
22 adequately their PII and medical information against hacking and/or disclosure to unauthorized
persons.

23 49. By accepting possession of the PII and medical information belonging to Plaintiff
24 and other members of the proposed classes, Defendant understood that Plaintiff and other
25 members of the proposed classes expected Defendant to safeguard adequately their PII and
26

1 medical information.

2 50. Defendant accepted possession of the PII and medical information belonging to
3 Plaintiff and other members of the proposed classes for the purpose of providing health
4 insurance and/or medical treatment to them. Thus, a bailment (or deposit) was established for
5 the mutual benefit of the parties.

6 51. During the time of bailment, Defendant owed Plaintiff and other members of the
7 proposed classes a duty to safeguard this information properly and maintain reasonable security
8 procedures and practices to protect such information.

9 52. Defendant breached this duty.

10 53. Plaintiff and the other members of the classes have suffered harm as a result of
11 Defendant's breach of its bailment and of its duty of care. These victims' loss of control over
12 the PII and medical information exposed subjects each of them to a greatly enhanced risk of
13 identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and
14 myriad other types of fraud and theft. Plaintiff and other members of the proposed classes
15 suffered and continue to suffer further harm by virtue of Defendant's failure to give timely and
16 complete notice to them concerning the Data Breach and the risks they face.

17 **FOURTH CAUSE OF ACTION**

18 **Breach of Contract**

19 **(On Behalf of Plaintiff and all Classes)**

20 54. Plaintiff incorporates by reference all other paragraphs alleged herein.

21 55. Defendant entered into written (or, in the alternative implied) contracts with
22 Plaintiff and the classes in which it agreed to provide health insurance in exchange for periodic
23 payments of premiums.

24 56. Under the terms of this contractual agreement, Defendant was obliged to
25 maintain the security of its insureds' PII and medical information, and to comply with HIPAA.

26 57. Defendant breached its contractual obligations by failing to secure and safeguard
the PII and medical information of Plaintiff and other members of the classes. Defendant

1 negligently maintained systems that it knew were vulnerable to a security breach, despite being
 2 made aware of these vulnerabilities any number of ways, including through the federal
 3 government's audit of those very systems. Defendant negligently stored PII and medical
 4 information in an unencrypted form on a single, highly vulnerable database.

5 58. Defendant continues to breach its contractual obligations by failing to share
 6 crucial, complete information with Plaintiff and other members of the classes in a timely
 7 manner.

8 59. Plaintiff and the other members of the classes have suffered harm as a result of
 9 Defendant's breach of contract. These victims' loss of control over the PII and medical
 10 information exposed subjects each of them to a greatly enhanced risk of identity theft, medical
 11 identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of
 12 fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to
 13 suffer further harm by virtue of Defendant's failure to give timely and complete notice to them
 14 concerning the Data Breach and the risks they face.

15 **FIFTH CAUSE OF ACTION**

16 **Breach of Fiduciary Duty**

17 **(On Behalf of Plaintiff and all Classes)**

18 60. Plaintiff incorporates by reference all other paragraphs alleged herein.

19 61. As the health insurance provider to Plaintiff and other members of the proposed
 20 classes, Defendant owed such persons a fiduciary duty, which included the duty to safeguard
 21 this information properly and maintain reasonable security procedures and practices to protect
 22 such information, and to keep Plaintiff and other members of the proposed classes fully
 23 informed in a timely manner regarding the Data Breach.

24 62. Defendant breached its fiduciary duties by failing to secure and safeguard the PII
 25 and medical information of Plaintiff and other members of the classes. Defendant negligently
 26 maintained systems that it knew were vulnerable to a security breach, despite being made aware
 of these vulnerabilities any number of ways, including through the federal government's audit of

1 those very systems. Defendant negligently stored PII and medical information in an
 2 unencrypted form on a single, highly vulnerable database.

3 63. Defendant continues to breach its fiduciary duties by failing to share crucial,
 4 complete information with Plaintiff and other members of the classes in a timely manner.

5 64. Plaintiff and the other members of the classes have suffered harm as a result of
 6 Defendant's breach of fiduciary duty. These victims' loss of control over the PII and medical
 7 information exposed subjects each of them to a greatly enhanced risk of identity theft, medical
 8 identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of
 9 fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to
 10 suffer further harm by virtue of Defendant's failure to give timely and complete notice to them
 11 concerning the Data Breach and the risks they face.

12 **SIXTH CAUSE OF ACTION**

13 **Violation of Washington's Data Disclosure Law, RCW § 19.255.010-020**

14 **(On Behalf of Plaintiff and all Classes)**

15 65. Plaintiff incorporates by reference all other paragraphs alleged herein.

16 66. Under RCW § 19.255.010, Defendant is required to disclose "any breach of the
 17 security of the data immediately following discovery" of a data breach, "in the most expedient
 18 time possible and without unreasonable delay."

19 67. Under RCW § 19.255.020, Defendant is required to exercise "reasonable care to
 20 guard against unauthorized access to" the PII and medical information disclosed in the Data
 21 Breach.

22 68. Defendant failed to disclose the Data Breach in the most expedient time possible,
 23 and failed to exercise reasonable care to prevent the Data Breach.

24 69. Plaintiff seeks damages as permitted by law, as well as injunctive relief. As of
 25 this filing, Defendant has not provided notice to victims of the Data Breach consistent with the
 26 requirements of Washington law, and it should be compelled to do so without delay.

SEVENTH CAUSE OF ACTION

Violation of the Washington Consumer Protection Act, RCW § 19.86 *et seq.*

(On Behalf of Plaintiff and all Classes)

70. Plaintiff incorporates by reference all other paragraphs alleged herein.

71. Defendant is a “person” within the meaning of the Washington Consumer Protection Act, RCW § 19.86.010(1), and conducts “trade” and “commerce” within the meaning RCW § 19.86.010(2).

72. Plaintiff and other members of the classes are “persons” within the meaning of RCW § 19.86.010(1).

73. Defendant’s failure to safeguard the PII and medical information disclosed in the Data Breach constitutes an unfair act that offends public policy, including as set forth in HIPAA and the state laws cited *supra*.

74. Defendant’s failure to promptly and fully notify Plaintiff and other members of the classes regarding the Data Breach is unfair because these acts or practices offend public policy, including as set forth in HIPAA and the state laws cited *supra*.

75. Defendant’s failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, causes substantial injury to Plaintiff and other members of the classes, is not outweighed by any countervailing benefits to consumers or competitors, and is not reasonably avoidable by consumers.

76. Defendant’s failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive and/or unscrupulous.

77. Defendant’s unfair acts or practices occurred in its trade or business and have and are capable of injuring a substantial portion of the public. Defendant’s general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are

ongoing and/or have a substantial likelihood of being repeated.

78. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff and other members of the classes suffered injury in fact.

79. Plaintiff and other members of the classes are entitled to an order enjoining the conduct complained of herein and ordering Defendant to take remedial measures to prevent similar data breaches; actual damages; treble damages pursuant to RCW § 19.86.090; costs of suit, including reasonable attorney fees; and such further relief as the Court may deem proper.

EIGHTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of Plaintiff and All Classes)

80. Plaintiff incorporates by reference all other paragraphs alleged herein.

81. If the Court finds Plaintiff's and other Class members' contracts with Defendant for protection of their PII and medical information invalid, non-existent, or otherwise unenforceable, Plaintiff and other Class members may be left without any adequate remedy at law.

82. Plaintiff and other Class members conferred a monetary benefit on Defendant in the form of fees paid for healthcare insurance. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and other Class members.

83. The fees that Plaintiff and other Class members paid to Defendant were supposed to be used by Defendant, in part, to pay for the costs of reasonable data management and security, including encryption of PII and medical information.

84. Under principles of equity and good conscience, Defendant should not be permitted to retain the money paid by Plaintiff and other Class members, because Defendant failed to implement reasonable cyber security measures that Plaintiff and other Class members paid for and that are mandated by HIPAA, by the state laws cited above, and by industry standards.

85. As a result of Defendant's conduct, Plaintiff and other Class members suffered

1 damages in the amount of the difference between the price they paid for Defendant's insurance
2 as promised and the actual diminished value of what they received.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Plaintiff makes the following prayer for relief, on behalf of himself
5 and the proposed classes:

- 6 a. An order certifying the proposed classes pursuant to Federal Rule of Civil
7 Procedure 23 and appointing Plaintiff and her counsel to represent the classes;
- 8 b. An order awarding Plaintiff and other Class members monetary relief, including
9 actual and statutory damages;
- 10 c. Equitable relief enjoining Defendant from engaging in the wrongful conduct
11 complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and
12 other Class members' PII and medical information, and from refusing to issue
13 prompt, complete and accurate disclosures to Plaintiff and other Class members;
- 14 d. Equitable relief compelling Defendant to utilize appropriate methods and policies
15 with respect to its data collection, storage, and safety practices and to disclose
16 with specificity to Class members the type of data compromised in the Data
17 Breach, and other information required under the laws cited herein;
- 18 e. Equitable relief requiring restitution and disgorgement of the revenues
19 wrongfully retained as a result of Defendant's wrongful conduct;
- 20 f. An award of costs of suit and attorneys' fees, as allowable by law;
- 21 g. An award of pre-judgment and post-judgment interest, as provided by law;
- 22 h. Leave to amend this Complaint to conform to the evidence produced at trial; and
- 23 i. Such other and further relief as this Court may deem just and proper.

24 **DEMAND FOR JURY TRIAL**

25 Plaintiff demands a trial by jury on all claims so triable.

26 Dated: April 2, 2015.

IDE LAW OFFICE

s/Matthew J. Ide, WSBA No. 26002

Matthew J. Ide, WSBA No. 26002

7900 SE 28th Street, Suite 500
Mercer Island, WA 98040
Tel. (206) 625-1326
email: mjide@yahoo.com

LITE DEPALMA GREENBERG, LLC
Katrina Carroll, Esq.*
211 West Wacker Drive
Suite 500
Chicago, IL 60606
Telephone: 312.750.1265
email: kcarroll@litedepalma.com

KYROS LAW OFFICES
Konstantine W. Kyros, Esq.*
17 Miles Road
Hingham, MA 02043
Telephone: (800) 934-2921
Facsimile: (617) 583-1905
kon@kyroslaw.com

[**pro hac vice* applications to be submitted]

Attorneys for Plaintiff & the Proposed Classes